Common Standards for Information Security Measures
for Government Agencies (FY 2018)
Comments of BSA | The Software Alliance
June 28, 2018

BSA | The Software Alliance (BSA)[1] welcomes this opportunity to provide our response to the draft Common Standards for Information Security Measures for Government Agencies (FY 2018) ("Common Standards"), published by the National center of Incident readiness and Strategy for Cybersecurity ("NISC").

BSA appreciates the Government of Japan's (GOJ) constant efforts to improve information security measures by GOJ agencies and related entities. BSA has worked closely with governments around the world in relation to the development of national cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively deter and manage cybersecurity threats whilst still protecting the privacy and civil liberties of citizens.

As a result of this experience, BSA has developed the "International Cybersecurity Policy Framework" ("BSA Framework").[2] The BSA Framework sets out a recommended model for a comprehensive national cybersecurity policy, referring to key elements of national cybersecurity policy including government procurement.[3]

In 2016, BSA submitted comments and recommendations for the "Common Standards for Information Security Measures for Government Agencies" (FY 2016). The sections relating to our comments remains mostly unchanged in the 2018 edition. We would like to take this opportunity to reiterate our concerns and recommendations here by attaching our previous submission. In light of the increasing evidence of the value of cloud computing to securely

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] The BSA International Cybersecurity Framework is available on-line at:
https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf
More information is available at https://bsacybersecurity.bsa.org/

[3] See BSA international Framework pages 11-12 (Government Procurement)

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 4360 5473
F +81 4360 5301
W bsa.org
Japan Representative Office

support government agency objectives, we encourage NISC to address these industry concerns in the 2018 edition.

We are specifically concerned that the section on cloud computing use (see Section 4.1.4) continues to imply that cloud computing and related services have enhanced risks. Such statements may create the misleading impression that risks of cloud computing are greater than on-premise IT system. It is also important to take into consideration the varying cloud service models such as private cloud, public cloud, and hybrid cloud, and as with on premises systems, the specific risks must be assessed based on the context for which they will be used.

We are also concerned about the suggestion of physical network separation as a solution, when it could increase risks by interfering with the benefits of real-time security updates (see Sections 5.2.1-(2)a).

Section 4.1.4-(1) b referring to location of where data will be stored could further be improved. The Common Standards should not require the specification of physical location as long as CSPs can ensure the safe and secure management of data in accordance with the governing law. These descriptions deter uptake of cloud computing technologies and services even as the GOJ seeks to promote them.

BSA will be happy to collaborate with NISC into the future and to discuss these comments in more detail. We appreciate the GOJ and NISC for providing this opportunity to respond to the 2018 edition of Common Standards and hope our comments will be useful in finalizing this document.

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 4360 5473
F +81 4360 5301
W bsa.org
Japan Representative Office

Common Standards for Information Security Measures
for Central Government, etc. 2016 Edition

Comments of BSA | The Software Alliance
July 4, 2016

BSA | The Software Alliance (BSA)[1] welcomes this opportunity to provide our response and recommendations for the draft Common Standards for Information Security Measures for Central Government, etc. 2016 Edition ("Common Standards"), published by the National Center of Incident Readiness and Strategy for Cybersecurity ("NISC").

BSA appreciates the Government of Japan's (GOJ) constant efforts to improve information security measures by GOJ agencies and related entities. Recognizing the critical importance of effective cybersecurity strategies and measures for the health and development of the digital economy, BSA advocates for effective cybersecurity and related policies in markets around the world. In 2015, BSA submitted comments and recommendations for the Common Standards for Information Security Measures for Central Government etc. 2014 Edition ("2014 Edition").[2] In our present comments, we reiterate important issues from before, and provide additional responses and recommendations for items new to the 2016 Edition of the Common Standards.

Our comments focus on the following issues:

- Using appropriate language so that the guidance recognizes the inherent security, functionality, support, and cost-savings advantages of cloud computing services over traditional on-premises information technology (IT) systems.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.
BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro and Workday.
[2] See our previous comments at http://bsa.or.jp/files/20140214.pdf

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

- Establishing systems by which cloud computing service providers may be evaluated based on their compliance with or certification to relevant international standards.
- Avoiding unnecessary requirements or recommendations that IT systems be physically separated from the Internet.

These comments are based on the fact that Internet-enabled services, such as cloud computing, are having a profound effect upon the global economy. Ensuring that governments enact policies that incentivize the development, deployment and adoption of such services is critical for enabling our societies to maximally benefit from these exciting developments. According to a report BSA recently published,[3] the processes to gather, store, analyze and transform data are at the heart of data innovation to derive immense value from the vast amounts of otherwise unproductive information, and data innovation is driving extraordinary worldwide progress on some of the world's toughest challenges.

The GOJ recognizes these trends and is attempting to seize their opportunities through initiatives such as the Japan Revitalization Strategy 2016 to improve the convenience of administrative services for citizens while driving down the operational costs by leveraging the latest technologies including cloud computing. BSA supports such leadership as BSA members are at the forefront of providing cutting-edge technologies and services, such as safe and secure cloud computing services, data analytics, and the devices and applications that underpin them.

In order to help society fully benefit from this innovation, it is critically important for governments and private enterprises to work together and share best practices on all IT policies including cybersecurity. It is also important for the government to lead by example. It is very important for the government to ensure that its cybersecurity guidance is effective, flexible, technology-neutral, risk-based, and does not create the misimpression that cloud computing services are inherently riskier than traditional on-premises IT systems. Based on this point of view, we respectfully provide the specific comments below, in order of priority.

Part 5 Lifecycle of Information Systems:

The objective of *Section 5.2.1 - Planning and Requirements of Information Systems*, to ensure information security throughout the entire lifecycle of an information system, is without objection. Indeed, the Common Standards state that one risk of failing to specify security requirements in information systems is "…increased costs associated with ***excessive information security measures***…" (emphasis added).

However, new language in *sub-section 5.2.1(2) – Establishing Information System Security Requirements*, requires that an information system security administrator shall determine

[3] What's the Big Deal With Data? http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf

"…whether or not to separate the information system to be built from the Internet or an information system that is connected to the Internet…". It is our view that physical separation of an information system from the Internet (thereby precluding, by definition, cloud computing and related Internet-enabled services) is usually an "excessive information security measure." We recognize that the Common Standards acknowledge that this decision should be made based on "the purpose of building the information system, business requirements of the target business operation, and classification of information to be handled in such information system…" and may not be intended to be the default choice. Separating an information system from the Internet would significantly reduce the ability to access and utilize information held in such a system and would not represent a fool-proof security solution. A multi-layered approach to cybersecurity defenses can provide effective protection against threats without cutting off connectivity and access to the Internet and the associated benefits and productivity gains. Indeed, a recent study reported that 31.5% of cyber-attacks were conducted by employees or former employees with malicious intent and 23.5% of the attacks were conducted by current employees.[4] Cutting an information system off from the Internet not only limits the accessibility and usability of any relevant data, but it also limits the government agency concerned from benefiting from the cutting edge security solutions employed by leading cloud computing service providers, such as BSA members.

Recommendation:

We urge the GOJ to delete the new references to separating information systems from the Internet (e.g. network separation) in sub-section 5.2.1(2)(a) and in the Guideline for Developing Measures Standards for the Central Government Agencies (2016 Edition) ("Guideline") (page 133). This will help ensure that the Common Standards do not inadvertently imply to public officials that network separation is the most effective way of securing an information system.

Part 4 Outsourcing:

Section 4.1.4 – Using Cloud Services is new to the 2016 Edition of the Common Standards and specifically addresses the security considerations of procuring cloud computing services. The Common Standards recognize the importance of government agencies embracing cloud computing services and are rightfully providing guidance regarding the factors that must be considered when adopting and utilizing a cloud computing solution. Most experts recognize that leading cloud service providers now offer much higher levels of security for user data than even highly sophisticated enterprises could provide on their own. Many cloud services allow users to encrypt the data they store in the cloud—meaning that even the cloud service provider itself cannot access the data in a readable form. It would be useful for the Common Standards to reference aspects of cloud computing services that provide enhanced security to

[4] IBM 2015 Cyber Security Intelligence Index
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

their users to counter the impression that cloud computing increases information security risk over alternatives.

In addition, we note a number of areas that could be improved to avoid confusion or misinterpretation.

Section 4.1.1 states that when considering the use of cloud computing, the subject matter of *Section 4.1.4* must be considered ***in addition*** to *Section 4.1.1* because "cloud services have inherent risks." As discussed above, while it may be factually correct to state that cloud services have "inherent risks", such a statement gives the misimpression that such risks are greater than alternatives, such as on-premises IT systems, which is simply not the case.

Specific to *Section 4.1.4*, sub-section (b) states that it is important to evaluate the "risks in which domestic and foreign laws may be applied to the information handled in the cloud service, and designate the implementation site of the outsourced service and the governing law and competent court…" BSA agrees that it is important to confirm governing laws, jurisdiction and applicable laws and regulations that may apply to data handled by cloud services. However, it is not necessary to specify the particular location where data resides, as long as the cloud service provider can ensure that the data will be handled and secured appropriately and in accordance with the governing law. Many of the advantages of cloud computing services derive from the mobility of data across international borders and imposing requirements to restrict such movement, or account for the "physical location" of data may limit the cloud computing services or providers without adding any additional security to the data. Data security does not ultimately depend on the physical location of the data. Instead, data security is a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data.

We also note that *Section 4.1.4* acknowledges that it can be difficult for an information system security administrator to directly confirm how information is being handled and *sub-sections 4.1.4(d-e)* rightfully requires the information system security administrator to take into consideration the "characteristics of a cloud service" and "prescribe the security requirements…taking an extensive view of the overall distribution channel of information so that security is appropriately ensured…". The administrator must also "comprehensively and objectively evaluate…the cloud service." The Guidelines on pages 118-119 reference information security management system (ISMS) authentication provided by ISO/IEC 27017 for cloud services as a relevant international standard, the cloud information security audit provided by the Japan Security Audit Association and the Service Organization Control Report, which is a certified report for internal controls regarding cloud service providers' security measures. BSA supports efforts to utilize voluntary international standards that have been

developed in a transparent and industry-led fashion as a powerful way to ensure the capabilities and qualities of technology-related products and services.

Recommendation:
BSA urges the GOJ to explicitly incorporate recognition of compliance with or certification to relevant international standards in the Common Standards to assist in determining the suitability of competing cloud computing service providers.

BSA also encourages GOJ to adopt cloud service accreditation systems for government agencies, akin to the Federal Risk and Authorization Management Program (FedRAMP) system adopted by the US Federal Government, which aims to provide a standardized approach to security assessment and authorization.

Together, these will help information system security administrators evaluate cloud computing service providers holistically, improving the likelihood that tenders will go to the most cost-effective, secure and functional cloud systems available for the need at hand. This in turn will promote the deployment of safe and effective cloud computing systems in the public sector and beyond.

Section 4.1.1 – Outsourcing and *Section 4.1.2 – Using External Services Based on Terms and Conditions* raise concerns about unduly limiting information that can be handled by third parties in part due to a lack of clarity or confusion regarding the different kinds of outsourced service providers. It appears that the blanket prohibition of handling "information requiring confidentiality" is limited to "external services based on terms and conditions."

Should there be a case where a cloud service can also be an "external service based on terms and conditions", it remains unclear whether such a cloud service would be able to handle confidential information due to the restrictions identified in *Sections 4.1.1* and *4.1.2*. According to *Section 1.3 – Definitions of Terms*, "Cloud Service" and "External service based on terms and conditions" are distinct concepts. The Guideline, on page 7, depicts the different kinds of outsourcing entities described under *Section 4.1*. However, responsible officials in government agencies may not notice this distinction and may be misled or confused.

In addition, *Section 4.1.1.2(b)(A)* refers to the need to accept "security audits." In the new *Section 4.1.4.1(e)*, the system security administrator is required to "comprehensively and objectively evaluate" the cloud service provider and outsourcing contractors "based on the contents of the information security audit report…and the status of application of various certification/authentication systems." In the past, BSA has raised concerns that the Common Standards appear to require, or encourage, on-site inspections by government officials as part of the audit process.

Recommendations:

BSA recommends that GOJ narrow the scope of applicability of "information requiring confidentiality" in the Common Standards to only the most sensitive information to ensure that the prohibition on using "external services based on terms and conditions" for handling such information is not overly broad.

BSA requests that the Common Standards should clarify that cloud computing services are not considered "external services based on terms and conditions." We suggest including the Guideline's explanation of different categories of outsourcing entities, such as the diagram on page 7, in the Common Standards.

BSA suggests that the Common Standards should be amended to clarify that the prohibitions applied to "external services based on terms and conditions" should only apply if the terms and conditions are insufficient to meet security and other requirements for "information requiring confidentiality."

Finally, BSA urges the GOJ to clarify that in order to verify whether or not an outsourcing entity, especially a cloud service provider, has acceptable security measures, the government should utilize various available information, including, without limitation, information concerning information security measures provided by a cloud service provider, an audit report regarding a cloud service provider by an independent party, and the status of compliance with international standards related to information security (see discussion on international standards in comments on *Section 4.1.4* above.). Cloud service providers should not require on-site inspections by government officials directly, as such measures are not practical or effective and would have the indirect consequence of requiring data/hardware localization.

Conclusion:

BSA would like to thank once again the GOJ and NISC for granting us the opportunity to provide these comments and recommendations on this important document. We hope they will be useful both as you finalize the Common Standards, but also more generally as you continuously work to enhance the cybersecurity capabilities of public and private sector IT systems and promote the adoption of Internet-enabled services, such as cloud computing, which have so much promise of spurring economic growth, creating employment and solving the difficult challenges our societies face.

Please let us know if you have any questions or would like to discuss these comments in more detail.